(19) **United States**

(12) **Patent Application Publication** (10) Pub. No.: **US 2001/0056535 A1**

VANSTONE et al. (43) Pub. Date: **Dec. 27, 2001**

(54) **LOG-ON VERIFICATION PROTOCOL**

(76) Inventors: SCOTT A. VANSTONE, WATERLOO ONTARIO (CA); DONALD JOHNSON, FAIRFAX, VA (US)

Correspondence Address:
J BENJAMIN BAI PH D
JENKENS & GILCHRIST P C
1100 LOUISIANA STE 1800
HOUSTON, TX 770025214

(*) Notice: This is a publication of a continued prosecution application (CPA) filed under 37 CFR 1.53(d).

Publication Classification

(57) **ABSTRACT**

A method and apparatus for authenticating a pair of correspondents C,S in an information exchange session to permit exchange of information therebetween. The first correspondent C having log on applets and the correspondent having means for processing applets. The method is characterized in that the first correspondent C transmitting to the second correspondent S a first unique information, the second correspondent S verifying the identity of C and generating a second unique information; transmitting to C the first and second unique information; the C verifying the first unique information to thereby establish currency of the session; the first correspondent C then generating a third unique information and transmitting the third unique information to the S along with an information request; the second correspondent S transmitting to C the requested information along with said second and third unique information; said c verifying said third unique information to thereby establish currency of the request and verifying the second unique information to thereby establish currency of the session; said C repeating steps the above steps for each additional information requested by C.

Figure 1

CLIENT

SERVER

generate x ~ 100

$H = h(ID_C \| PU_{CA} \| x)$ ~102

$s = S_{PRC}(H)$ ~ 103

ID_C , PU_{CA} , x, s ~104

check PU_{CA} 112

extract PU_C 113   or   Look up PU_C 113'

$V_{PU_c}(s)$ ~ 114

generate y ~ 116

Verify Cert$_s$ ~124

Verify x ~ 125

Extract PU$_s$ ~126

$V_{PU_c}(s')$ ~127

Store y ~ 129

$H' = h(\text{log-on-applet} \| x \| y \| ID_C)$ 118

$s' = S_{PR_s}(H')$ 120

log-on-applet , y, s', cert$_s$ 122

Figure 2

client   server

Generate z — 210

applet _ ID — 212

z . applet _ ID — 214

216

$H'' = h\ (\text{applet} \parallel y \parallel z \parallel ID_C)$

$s' = S_{PR_C}\ (H')$ — 218

applet, s'' — 220

$V_{PU}\ (s'')$ — 222

Verify y — 223

Verify z — 224

Next applet
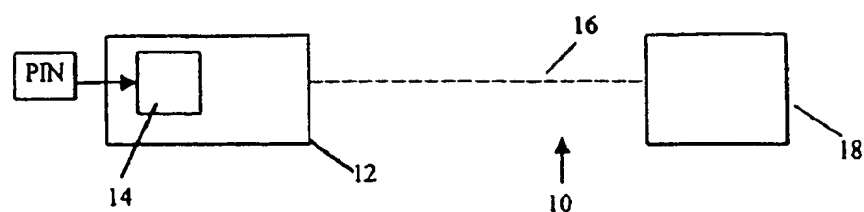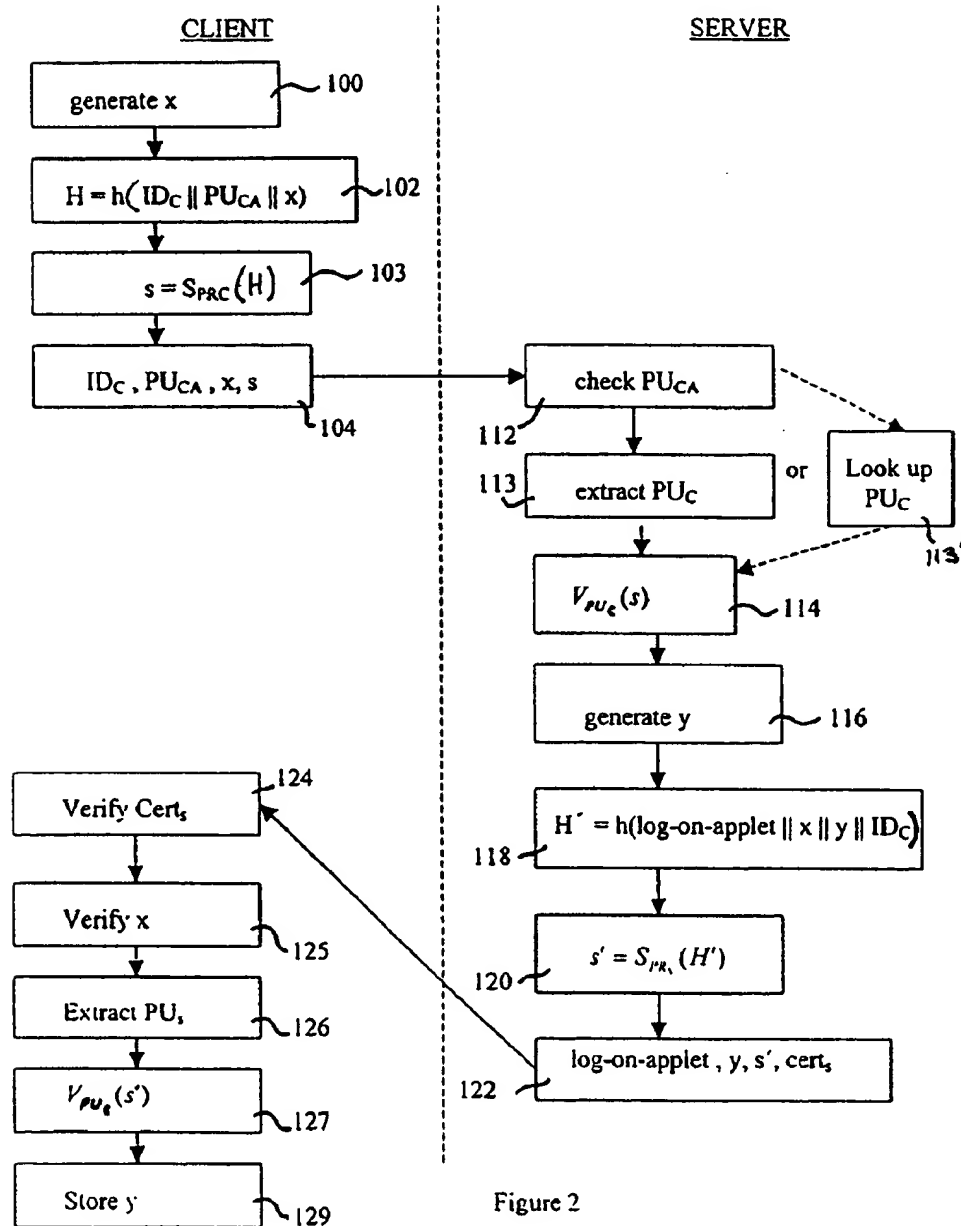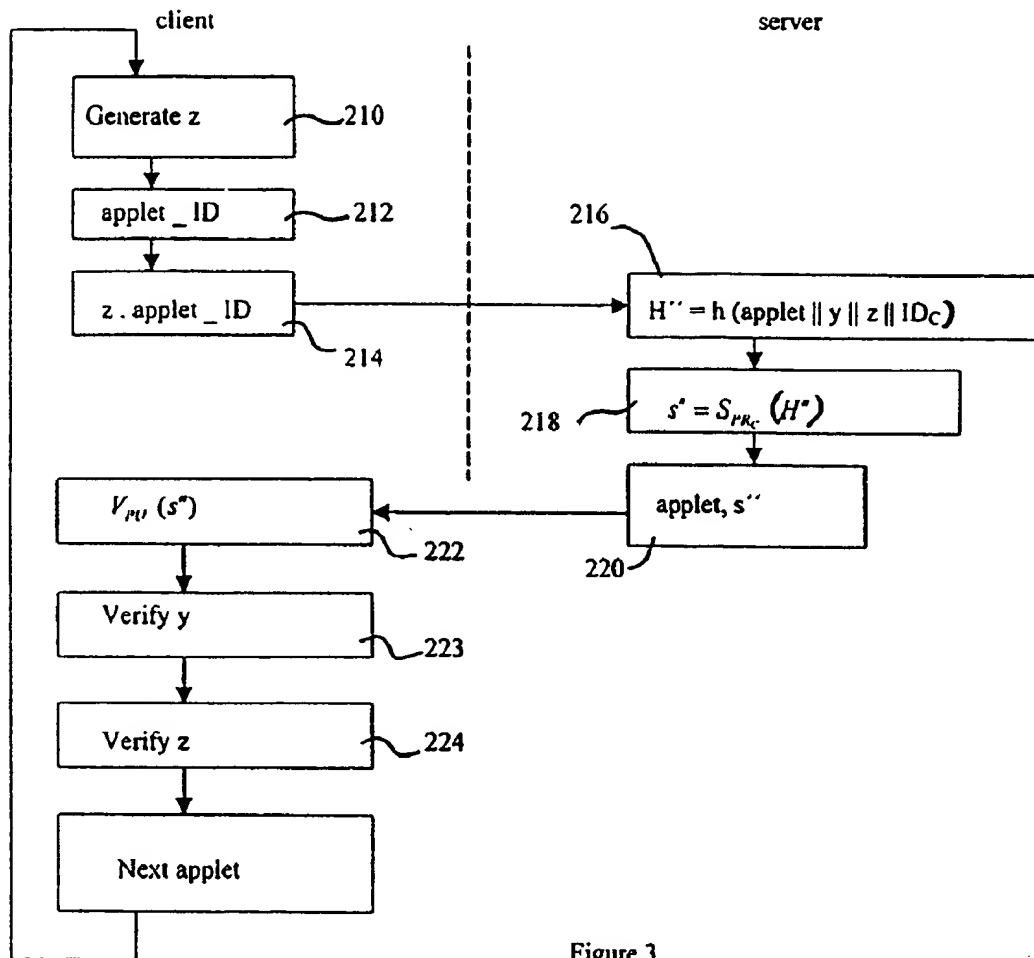
Figure 3

LOG-ON VERIFICATION PROTOCOL

[0001] This is a continuation of PCT/CA98/00417, which was filed on May 4, 1998.

FIELD OF THE INVENTION

[0002] The invention relates to a protocol for the secure receipt and transmission of data between a pair of correspondents and in particular for the secure receipt of data by a client in a client-server environment.

BACKGROUND OF THE INVENTION

[0003] With the advent of the Internet and the proliferation of Internet users along with the dramatic increase in data baud rates, there has been a move to distributed computing. For example, in the windows environment, a browser may be used to access a website and download a HTML page. Within the page might be included a program applet much like an image that is contained within the page. The applet's code is transferred from the server to the client system and executed by the client's computer. There are also instances where software or program applets are provided from a server to a client.

[0004] In the cases where the client does not trust the server a protocol has to be implemented whereby the client is able to authenticate the server. Or more generally where the client does not know the server since the server will serve any client, i.e. any requester is potentially valid as far as the client is concerned. Furthermore the applets received from the server include in some instances a log-on applet received from the server. Thus there exists a need for a log-on applet authentication protocol. The documents titled "Security Defects in CCITT Recommendation X.509-The Directory Authentication Framework", "Elliptic Curves Over F_p Suitable For Cryptosystems", "Secure User Access Control For Public Networks", and U.S. Pat. No. 5,434,918 are referenced as background art.

SUMMARY OF THE INVENTION

[0005] This invention seeks to provide a solution to the problem of server verification by a client.

[0006] According to an aspect of this invention there is provided a method of authenticating pair of correspondents C,S in an information exchange session to permit exchange of information there between, characterized in that:

[0007] a) the first correspondent C transmitting to the second correspondent S a first unique information,

[0008] b) the second correspondent S verifying the identity of C and generating a second unique information;

[0009] c) transmitting to C the first and second unique information;

[0010] d) the C verifying the first unique information to thereby establish currency of the session;

[0011] e) the first correspondent C then generating a third unique information and transmitting the third unique information to the S along with an information request;

[0012] f) the second correspondent S transmitting to C the requested information along with said second and third unique information;

[0013] g) said c verifying said third unique information to thereby establish currency of the request and verifying the second unique information to thereby establish currency of the session;

[0014] h) said C repeating steps e) to g) for each additional information requested by C.

[0015] Also, this aspect of the invention provides for apparatus for carrying out the method. Such an apparatus can comprise any computational apparatus such as a suitably programmed computer.

DESCRIPTION OF THE DRAWINGS

[0016] These and other advantages of the present invention will become more apparent from the following discussion of preferred embodiments of the invention which are described by way of example only and with reference to the accompanying drawings in which like elements have been assigned like reference numerals and where:

[0017] FIG. 1 is a schematic diagram of a client server configuration;

[0018] FIG. 2 is a schematic diagram showing server authentication; and

[0019] FIG. 3 is a schematic diagram showing applet authentication.

DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[0020] Referring to FIG. 1, a typical arrangement in which the protocol may be implemented is shown generally numeral 10. A client 12 includes a hardware token 14 and connects via a suitable communication channel 16 to a server 18. The hardware token 14 maybe PIN activated and includes a root certifying authority (CA) public key, PU_{CA}, a client private key, PR_C, and an ECDSA (elliptic curve digital signature algorithm) signing software. It may be noted that the hardware token may also be mimicked or implemented in software.

[0021] In addition to the hardware token, the client has stored therein an identification of the client, ID_C, wherein some cases the ID could be the certificate of the client containing the public key PU_C of the client. Alternatively the certificate may contain only the identity ID_C of the client. This identity may then be used as an index into a look-up table of public keys stored in the server. Additionally, the client includes a hash function such as SHA-1, an elliptic curve DSA (ECDSA) verification software, and optionally MQV (Menezes-Qu-Vanstone) key exchange algorithm software and a DES (Data Encryption Standard) or TDES (Triple DES) encryption algorithms which are used to encrypt and/or authenticate applets from the server.

[0022] The server includes log-on applets, crypto software and other applets. The server also includes a private key PR_S and a certificate $CERT_S$ which includes its public key PU_S. Optionally the server may also include a database of client public keys indexed by a client identification.

[0023] Referring now to FIG. 2, when the client 12 wishes to request an applet from a server for the first time, the client first authenticates the server by generating a random number x 100, preferably on the hardware token 14. A counter or a time stamp or the like may generate the value x. A hash H on the concatenation of the client identification ID_C, the root public key and x is computed 102. A signature s of the hash

H is calculated using the client private key PR_C **103**. The client then sends a request **104** containing ID_C, PU_{CA}, x, s to the server **18**. The client to indicate the currency of the transaction of session uses the value x.

[0024] The server then checks that root certifying authority public key PU_{CA} is correct **112**. The client public key PU_c is either extracted **113** from the certificate or a lookup **113**' is performed in the server database. The signature s is then verified **114** using PU_C.

[0025] The server then generates a random number y **116** and computes the hash H'**118** on the concatenated message of the log of the applet, x, y and ID_C. A signature s' on the hash H' is computed using the server private key PR_S **120**. A response **122** is sent to the client and includes the log-on applet, y, s' and the server's certificate $CERT_S$. Once the client receives this information it verifies the validity of $CERT_s$ **124**. The client also verifies x **125**, which was sent back with the message from the server and thus indicating the currency of the session. The public key of the server PU_S is extracted from the certificate **126** and used to verify the signature s'**127**. This then verifies the server to the client. The value y is also extracted saved by the client **129** to be used in later transactions.

[0026] Turning to **FIG. 3**, once the client has verified the server it may then request an appropriate applet by first generating a random number z **210**. A request **214** is then sent to the server which includes an identification of the appropriate applet **212** and the random number z. The server then computes a hash H" on the concatenation of the applet, y, z and ID_C **126**. The server then computes a signature s"**218** on the hash H" using the private key of the server PR_C. Both the applet and the signature s" are then sent to the client **220**. The client verifies the signature **222** using the server public key and once verified may safely use the applet. The value$_y$ is also verified **223** to establish currency of the session Th value$_z$ is also checked **224**o make sure it is current. If the client requires more applets, steps **210** and **224** are repeated for a given session. When a new session is resumed the client may re-authenticate the server as set out in **FIG. 2**.

[0027] While the invention has been described in connection with a specific embodiment thereof and in a specific use, various modifications thereof will occur to those skilled in the art without departing from the essence of the invention.

[0028] The terms and expressions which have been employed in the specification are used as terms of description and not of limitations, there is no intention in the use of such terms and expressions to exclude any equivalents of the features shown and described or portions thereof, but it is recognized that various modifications are possible within the scope of the invention.

What is claimed is:

1. A method of authenticating pair of correspondents (C,S) in an information exchange session to permit exchange of information therebetween, the method characterized in that:

a) the first correspondent (C) transmitting to the second correspondent (S) a first unique information,

b) the second correspondent (S) verifying the identity of the first correspondent (C) and generating a second unique information;

c) transmitting to the first correspondent (C) the first and second unique information;

d) the first correspondent (C) verifying the first unique information to thereby establish currency of the session;

e) the first correspondent (C) then generating a third unique information and transmitting the third unique information to the second correspondent (S) along with an information request;

f) the second correspondent (S) transmitting to the first correspondent (C) the requested information along with said second and third unique information;

g) said first correspondent (C) verifying said third unique information to thereby establish currency of the request and verifying the second unique information to thereby establish currency of the session;

h) said first correspondent (C) repeating steps e) to g) for each additional information requested by the first correspondent (C).

2. A method as defined in claim 1, said unique information being a random number x.

3. A method as defined in claim 2, said first correspondent (C) including a hardware token for generating said random number.

4. A data communication system for providing exchange of authenticated information between a pair of correspondents (C,S) in an information exchange session, said system comprising:

a) said first correspondent (C) including a hardware token having a public key, a private key and ECDSA program; said program for

i) transmitting to the second correspondent (S) a first unique information,

ii) the second correspondent (S) verifying the identity of the first correspondent (C) and generating a second unique information;

iii) transmitting to the first correspondent (C) the first and second unique information;

iv) the first correspondent (C) verifying the first unique information to thereby establish currency of the session;

v) the first correspondent (C) then generating a third unique information and transmitting the third unique information to the second correspondent (S) along with an information request;

vi) the second correspondent (S) transmitting to of the first correspondent (C) the requested information along with said second and third unique information;

vii) said first correspondent (C) verifying said third unique information to thereby establish currency of the request and verifying the second unique information to thereby establish currency of the session;

viii) said first correspondent (C) repeating steps v) to vii) for each additional information requested by of the first correspondent (C).

5. A system for authenticating pair of correspondents (C,S) in an information exchange session, to permit exchange of information therebetween, the system characterized in that:

a) means for transmitting by the first correspondent (C) to the second correspondent (S) a first unique information,

b) means for verifying the identity of the first correspondent (C) by the second correspondent (S) and generating a second unique information;

c) means for transmitting to the first correspondent (C) the first and second unique information;

d) means for verifying the first unique information by the first correspondent (C) to thereby establish currency of the session;

e) means for generating a third unique information and transmitting the third unique information to the second correspondent (S) along with an information request;

f) means for transmitting to the first correspondent (C) the requested information along with said second and third unique information;

g) means for verifying said third unique information to thereby establish currency of the request and verifying the second unique information to thereby establish currency of the session;

h) means for successively requesting additional information by said correspondent the first correspondent (C).

* * * * *